

FORM-PTO-1390  
(Rev. 12-29-99)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

**TRANSMITTAL LETTER TO THE UNITED STATES  
DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A FILING UNDER 35 U.S.C. 371**

032326-134

U.S. APPLICATION NO. (if known, see 37 C.F.R. 1.51)

Unassigned  
09/807614INTERNATIONAL APPLICATION NO.  
PCT/FR99/02521

INTERNATIONAL FILING DATE

15 October 1999

PRIORITY DATE CLAIMED

16 October 1998

TITLE OF INVENTION

ELECTRONIC COMPONENT FOR MASKING EXECUTION OF INSTRUCTIONS OR DATA MANIPULATION

APPLICANT(S) FOR DO/EO/US

Philippe ANGUIA and David NACCACHE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
  - a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
  - b. ☒ has been transmitted by the International Bureau.
  - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
  - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
  - b. ☐ have been transmitted by the International Bureau.
  - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
  - d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
  - ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

U.S. APPLICATION NO. (If known) <b>097/807614</b> Unassigned	INTERNATIONAL APPLICATION NO. <b>PCT/FR99/02521</b>	ATTORNEY'S DOCKET NUMBER <b>032326-134</b>
---	--	---


17. <input checked="" type="checkbox"/> The following fees are submitted:		<b>CALCULATIONS</b>	PTO USE ONLY
<b>Basic National Fee (37 CFR 1.492(a)(1)-(5)):</b>  Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO ..... \$1,000.00 (960)  International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ..... \$860.00 (970)  International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... \$710.00 (958)  International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) ..... \$690.00 (956)  International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) ..... \$100.00 (962)			
<b>ENTER APPROPRIATE BASIC FEE AMOUNT =</b>		<b>\$ 860.00</b>	
Surcharge of <b>\$130.00 (154)</b> for furnishing the oath or declaration later than months from the earliest claimed priority date (37 CFR 1.492(e)).		20 <input type="checkbox"/> 30 <input type="checkbox"/> \$ -0-	
Claims	Number Filed	Number Extra	Rate
Total Claims	15 -20 =	-0-	X\$18.00 (966)
Independent Claims	1 -3 =	-0-	X\$80.00 (964)
Multiple dependent claim(s) (if applicable)		+ \$270.00 (968)	\$ -0-
<b>TOTAL OF ABOVE CALCULATIONS =</b>		<b>\$ 860.00</b>	
Reduction for 1/2 for filing by small entity, if applicable (see below).		\$ -0-	
<b>SUBTOTAL =</b>		<b>\$ 860.00</b>	
Processing fee of <b>\$130.00 (156)</b> for furnishing the English translation later than months from the earliest claimed priority date (37 CFR 1.492(f)).		20 <input type="checkbox"/> 30 <input type="checkbox"/> \$ -0-	
<b>TOTAL NATIONAL FEE =</b>		<b>\$ -0-</b>	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). <b>\$40.00 (581)</b> per property +		\$ -0-	
<b>TOTAL FEES ENCLOSED =</b>		<b>\$ 860.00</b>	
		Amount to be: refunded \$	
		charged \$	

- a. ☐ Small entity status is hereby claimed.
- b. ☒ A check in the amount of \$ 860.00 to cover the above fees is enclosed.
- c. ☐ Please charge my Deposit Account No. 02-4800 in the amount of \$ \_\_\_\_\_ to cover the above fees. A duplicate copy of this sheet is enclosed.
- d. ☐ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

**NOTE:** Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre  
 BURNS, DOANE, SWECKER & MATHIS, L.L.P.  
 P.O. Box 1404  
 Alexandria, Virginia 22313-1404  
 (703) 836-6620



SIGNATURE

James A. LaBarre

NAME

28,632

REGISTRATION NUMBER

Patent  
 Attorney's Docket No. 032326-134

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of	)	
	)	
Philippe ANGUITA et al	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: April 16, 2001	)	
	)	
For: ELECTRONIC COMPONENT FOR	)	
MASKING EXECUTION OF	)	
INSTRUCTIONS OR DATA	)	
MANIPULATION	)	

**PRELIMINARY AMENDMENT**

Assistant Commissioner for Patents  
 Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

**IN THE SPECIFICATION:**

Page 1, immediately following the title appearing on lines 1 and 2, insert the following:

--This disclosure is based upon, and claims priority from French Application No. 98/12988, filed on October 16, 1998 and International Application No. PCT/FR99/02521, filed October 15, 1999, which was published on April 27, 2000 in a language other than English, the contents of which are incorporated herein by reference.

**Background of the Invention--**

Page 2, between lines 12 and 13, insert the following heading:

--Summary of the Invention--.

Page 3, between lines 25 and 26, insert the following heading:

--Brief Description of the Drawings--.

Page 4, between lines 2 and 3, insert the following heading:

--Detailed Description--.

**IN THE CLAIMS:**

Kindly replace claims 1-15, as follows.

1. (Amended) An electronic component including at least one microprocessor and storage means for executing a main program, and a counter for counting a random value, said counter generating an information signal at the end of a time period determined by said random value, for suspending the execution of said main program for a length of time required for a secondary program to be executed by the microprocessor.

2. (Amended) An electronic component according to claim 1, wherein the execution time of the secondary program is constant.

3. (Amended) An electronic component according to claim 1, wherein the execution time of the secondary program is variable.

4. (Amended) An electronic component according to claim 3, wherein the execution time of the secondary program is random.
5. (Amended) An electronic component according to claim 1, further including current-consuming means that are activated by the secondary program.
6. (Amended) An electronic component according to claim 5, wherein said current-consuming means comprise a charge pump.
7. (Amended) An electronic component according to claim 5, wherein said current-consuming means comprise instructions resulting in instantaneous consumption.
8. (Amended) A method of masking operations in an electronic component including at least one microprocessor and storage means for executing a main program, said method including the steps of generating a random value and suspending the execution of the main program at random instants based upon said random value for a length of time required for a secondary program to be executed.
9. (Amended) A method according to claim 8, wherein the secondary program comprises the steps of disabling a counter which determines said random instants, drawing a new random value, initializing the counter with said new value, and enabling the counter to resume counting before returning to the execution of the main program.

10. (Amended) A method according to claim 8, wherein the secondary program is executed in a random amount of time.

11. (Amended) A method according to claim 10, wherein the secondary program comprises the steps of disabling a counter which determines said random instants, drawing a new random value, counting down to zero from said new random value in a loop of the secondary program, drawing another new random value, initializing the counter to said other new value, and activating the counter, before returning to the execution of the main program.

12. (Amended) A method according to claim 8, wherein the secondary program also activates current-consuming means.

13. (Amended) A method according to claim 12, wherein said current-consuming means comprise a charge pump.

14. (Amended) A method according to claim 12 wherein said current-consuming means comprise instructions causing instantaneous current consumption.


15. (Amended) A method according to claim 8, further including the step of selecting one of a plurality of secondary programs to be executed during said suspending step.

**REMARKS**

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By:   
James A. LaBarre  
Registration No. 28,632

P.O. Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620

Date: April 16, 2001

**Attachment to Preliminary Amendment dated April 16, 2001**

**Marked-up Claims 1-15**

1. (Amended) An electronic component including at least one microprocessor [(1)] and storage means [(2, 3)] for executing a main program, [said electronic component being characterized in that it further includes] and a counter [(4)] for counting a random value [(R)], said counter generating [as output an end-of-counting] an information signal [(ITO)] at the end of a time period determined by said random value. for suspending the execution of said main program for [the] a length of time required for a secondary program to be executed by the microprocessor.

2. (Amended) An electronic component according to claim 1, [characterized in that] wherein the execution time of the secondary program is constant.

3. (Amended) An electronic component according to claim 1, [characterized in that] wherein the execution time of the secondary program is variable.

4. (Amended) An electronic component according to claim 3, [characterized in that] wherein the execution time of the secondary program is random.

5. (Amended) An electronic component according to [any preceding claim, characterized in that it further includes] claim 1, further including current-consuming means that are activated by the secondary program.



**Attachment to Preliminary Amendment dated April 16, 2001**

**Marked-up Claims 1-15**

6. (Amended) An electronic component according to claim 5, [characterized in that the] wherein said current-consuming means comprise a charge pump [(9)].

7. (Amended) An electronic component according to claim 5 [or 6], [characterized in that said] wherein said current-consuming means comprise instructions resulting in instantaneous consumption.

8. (Amended) A method of masking [the execution of] operations [or the handling of data] in an electronic component [(CI)] including at least one microprocessor [(1)] and storage means [(2, 3)] for executing a main program, said method [being characterized in that it consists in using a counter (4) and a random generator (5) for] including the steps of generating a random value [(R) to suspend] and suspending the execution of the main program at random instants based upon said random value for a length of [for the] time required for a secondary program to be executed.

9. (Amended) A method according to claim 8, [characterized in that] wherein the secondary program [consists in] comprises the steps of disabling [the] a counter which determines said random instants. [(4), in] drawing a new random value, [(R), in] initializing the counter [(4)] with said new value, and [in] enabling the [count-down] counter to resume counting before returning to the execution of the main program.

**Attachment to Preliminary Amendment dated April 16, 2001**

**Marked-up Claims 1-15**

10. (Amended) A method according to claim 8, [characterized in that] wherein  
the secondary program [can be] is executed in a random amount of time.

11. (Amended) A method according to claim 10, [characterized in that] wherein  
the secondary program [consists in] comprises the steps of disabling [the] a counter which  
determines said random instants. [(4), in] drawing a new random value, [(R), in] counting  
down to zero from said new random value in a loop of the secondary program, [then in]  
drawing another new random value, [(R), in] initializing the counter to said other new  
value, and [in] activating the counter, before returning to the execution of the main  
program.

12. (Amended) A method according to [any one of claims 8 to 11, characterized  
in that] claim 8, wherein the secondary program also activates current-consuming means.

13. (Amended) A method according to claim 12, [characterized in that] wherein  
said current-consuming means comprise a charge pump [(9)].

14. (Amended) A method according to claim 12 [or 13, characterized in that  
said] wherein said current-consuming means comprise instructions causing instantaneous  
current consumption.

**Attachment to Preliminary Amendment dated April 16, 2001**

**Marked-up Claims 1-15**

15. (Amended) A method according to [any one of claims 8 to 14, characterized in that it comprises various] claim 8, further including the step of selecting one of a plurality of secondary programs to be executed during said suspending step.

032326-134-0000

1/2/85

09/807614

JC03 Rec'd TGT/FNJ

16 APR 2001

ELECTRIC COMPONENT FOR MASKING EXECUTION OF  
INSTRUCTIONS OR DATA MANIPULATION

5 The present invention relates to an electronic component and to a method for masking the execution of instructions or the handling of data.

10 The present invention relates more particularly to electronic components used in applications in which access to services or to data is strictly controlled. Such a component has an architecture formed around a microprocessor and memories. It implements algorithms using secret data that is contained in the component and that is inaccessible from the outside. Such secret data can thus serve to validate or enable an electronic transaction such as a purchase, without said data being  
15 accessible from outside the component at any time.

20 However, by observing certain external parameters, such as the data interchanged with an external system, or the current consumed on the power supply terminal of the component, it is possible in some cases to retrieve information concerning the component by means of statistical processing. In particular, by observing the information flowing over the data bus (which is in

general a series bus) as a function of time, it is possible to obtain a correlation between said information and the procedure of the algorithm implemented in the component.

5           It may also be possible to obtain a correlation of said information with the observed current consumption as a function of time. It is then possible to deduce therefrom the value of a bit handled in an instruction. It is known that, at a given instant, the current  
10 consumed by a particular instruction varies depending on whether the value of the bit being handled is "0" or "1".

15           An object of the present invention is to mask the execution of instructions or the handling of data in the component, so as to make any observation of external parameters of the electronic component fruitless.

20           In the invention, provision is made to interrupt randomly the execution of the main program implemented by the electronic component so as to execute a secondary program. In this way, the procedure of the program changes all the time. Seen from the outside, it is no longer possible to perform statistical processing because the curves recorded are all offset  
25 randomly in time. For example, if the interchanged data is observed, the response time taken by the card to respond to any external command changes all the time, so that it is no longer possible to deduce therefrom any pertinent information.

30           As regards observing the consumed current, such current consumption over time is itself cut up and

diffused relative to the normal consumption curve, so that no pertinent information can be obtained from it.

Thus, as characterized, the invention provides an electronic component including at least one  
5 microprocessor and storage means for executing a main program.

According to the invention, the electronic component further includes a counter for counting a random value, said counter generating as output an end-of-counting information signal for suspending the  
10 execution of said main program for the time required for a secondary program to be executed by the microprocessor.

In an embodiment of the invention, the execution time of the secondary program is constant. In another  
15 embodiment of the invention, said execution time is variable. It may even be random.

In an improved embodiment, provision is made for the secondary program to activate current-consuming  
20 means so that they distort the current consumption curve of the component, thereby masking the executed operations and the handled data even more effectively.

The invention also provides a method of masking the execution of operations or the handling of data in an  
25 electronic component.

Other characteristics and advantages of the invention are described in more detail in the following description given by way of non-limiting example and with reference to the accompanying drawing, in which:

30 Figure 1 is a block diagram of a variant of an electronic component of the invention; and

Figure 2 shows a variant of the block diagram of a variant of an electronic component of the invention.

Figure 1 is a simplified block diagram of an electronic component CI of the invention. It includes a microprocessor 1 and internal resources which are connected to a data bus 6. The internal resources are constituted, in particular, by memories, and, in the example shown, by a program memory 2 and a working memory 3, by a counter 4, and by a random generator 5 for generating a random value R.

The electronic component CI includes various external connection terminals. In the example shown, it is a series data input/output component and therefore has a data input/output terminal I/O. It also has a ground terminal Vss, a power supply terminal Vcc, and terminals relating to control signals (not shown).

The microprocessor receives instructions and data via a series input/output port 8 connected to the data input/output terminal in association with an external system.

The microprocessor internally generates various control signals for managing the various internal resources.

Among these control signals, an enable signal EN for enabling the counter 4 is shown, as is a load signal LOAD for initializing the counter, and a select signal SEL for activating the random generator 5.

When it is enabled (EN activated), the counter generates an end-of-counting signal ITO. This end-of-counting information signal is used as a signal for interrupting the microprocessor. It is thus connected

to an input of the interrupt port 7 of the microprocessor. It should be noted that the expression "end-of-counting" is a general expression which means either that the counter has finished counting up to a determined value or that the counter has finished counting down to zero from a determined value.

It should be noted that, in the example more particularly shown, the counter is a hardware resource.

The microprocessor 1 executes a main program contained in the program memory and relating to data or instructions received from the series input/output port 8, in association with an external system.

In the invention, the execution of the main program is suspended at random moments, while a secondary program (contained in the program memory) is being executed.

For this purpose, at the start of the main program, a routine for initializing the counter with a new random value is provided. In practice, this routine comprises instructions for disabling the counter (EN deactivated), drawing a random value R from the random generator 5, loading (LOAD) this value in the counter, and then activating the counter (EN activated).

Once the counter has counted down to zero, it activates the end-of-counting information signal ITO, thereby causing an interruption at the microprocessor. Execution of the main program is suspended for the time necessary for the microprocessor to execute the secondary program, corresponding to the routine for managing the interruption in question.



The secondary program comprises at least the above-described sequence for initializing the counter, to a new random value, so that a new interruption can take place.

5        This secondary program may correspond to a fixed number of instructions. In which case, it is executed in constant time. For example, if the secondary program comprises only the instructions corresponding to drawing a new random value R from the generator 5 and to loading said new value R into the counter 4 (initialization), the secondary program can be executed  
10        in constant time.

      In which case, in addition to executing the main program, pieces of code (corresponding to the secondary  
15        program) are executed in constant time at random moments.

      In a variant of the invention, provision is made for the execution duration of the secondary program to be variable.

20        In a first practical embodiment, the second program provides a test on an item of binary data that is modified each time it goes through the program, the number of instructions executed then being a function of the result of the test. It is thus possible for the  
25        variable execution duration to depend on a mathematical function. For example, if the mathematical function requires a certain number of computation turns to reach the result, this number of turns being a function of the input data, the execution duration is variable,  
30        dependent on a mathematical function. All these techniques to reach a variable duration are well known.

In another practical embodiment, provision is made for the variable execution duration to be random. In this embodiment, provision is made for the secondary program to comprise disabling the counter, drawing a new random value, counting down to zero from said value in a count-down loop, and then initializing the counter to a new random value.

In this variant, pieces of code executed in random time at random moments are inserted into the execution of the main program.

In practice, numerous variants of the invention are possible.

In particular, in order to avoid degrading the execution time of the main program too much, it is possible to make provision to limit in time the total duration of delays due to executing the secondary program(s).

In another embodiment of the invention, provision is made not only to suspend execution of the main program at random moments, but also to make provision for additional current consumption, which "scrambles" the current consumption due to the execution of the main program.

This additional current consumption can be due instantaneously to instructions provided in the secondary program. For example, it is possible to make provision in the secondary program to execute computation turns of an algorithm, e.g. a cryptography algorithm.

This execution corresponds to an instantaneous current consumption, i.e. the execution time of the instruction, which scrambles the normal consumption of

the main program by being interposed in the normal current consumption as a function of the time due to the execution of the main program.

It is also possible to make provision for this additional current consumption to have a lasting effect for a certain length of time. The secondary program then makes provision to activate the current-consuming means, which consume current for at least a certain length of time, during the execution of the following instructions of the secondary program and of the main program.

A block diagram of an electronic component corresponding to this second embodiment of the invention is shown in Figure 2.

In addition to the above-described elements that bear the same references as in Figure 1, the electronic component includes a charge pump 9.

This charge pump is normally organized to deliver a high voltage  $V_{pp}$  for programming and/or erasing purposes from the power supply voltage  $V_{cc}$  so as to make it possible to program and/erase data in an electrically programmable and/or erasable read-only memory, such as, for example, memories commonly referred to as "EPROMs", "EEPROMs", or "flash EPROMs". In the invention, this charge pump is associated with the program memory.

In the example, it is activated by a write signal WE from the program memory.

Such a pump has the known characteristic of consuming a large amount of current during the time required to establish the high voltage at the output, and during the time required for the programming or for

the erasure, which time may be approximately a few milliseconds. By activating such a pump, e.g. by providing a programming instruction in the secondary program, high current consumption is superimposed, thereby masking the consumption of the following instructions of the secondary program and of the main program.

The invention is not limited to the above-described embodiments and variants. It covers any use of means for suspending the main program at random instants for a time that may be fixed, variable, or random, with or without means being used for adding additional current consumption.

With such masking or scrambling, by using any of the variants of the invention, or a combination thereof, no statistical processing is possible.

In practice, the choice of secondary program may depend on the application for which the electronic component is designed.

The invention applies to all components including at least one counter and a random generator. For any given electronic component, the choice of secondary program depends on the resources of the component in question, and on the effectiveness as regards the application in question.

It is also possible to use various secondary programs, which makes it possible to mix types, so as to improve the scrambling, the choice of the secondary program to be executed then being made at the beginning of the interruption routine.

Such a component is particularly well suited for use in chip cards or "smart cards", so as to improve tamper-proofing of them.

## CLAIMS

1. An electronic component including at least one microprocessor (1) and storage means (2, 3) for  
5 executing a main program, said electronic component being characterized in that it further includes a counter (4) for counting a random value (R), said counter generating as output an end-of-counting information signal (ITO) for suspending the execution  
10 of said main program for the time required for a secondary program to be executed by the microprocessor.

2. An electronic component according to claim 1, characterized in that the execution time of the secondary program is constant.

3. An electronic component according to claim 1, characterized in that the execution time of the secondary program is variable.

4. An electronic component according to claim 3, characterized in that the execution time of the  
20 secondary program is random.

5. An electronic component according to any preceding claim, characterized in that it further includes current-consuming means that are activated by the secondary program.

6. An electronic component according to claim 5, characterized in that the current-consuming means comprise a charge pump (9).

7. An electronic component according to claim 5 or 6, characterized in that said means comprise  
30 instructions resulting in instantaneous consumption.

8. A method of masking the execution of operations or the handling of data in an electronic component (CI)

including at least one microprocessor (1) and storage means (2, 3) for executing a main program, said method being characterized in that it consists in using a counter (4) and a random generator (5) for generating a random value (R) to suspend the execution of the main program at random instants for the time required for a secondary program to be executed.

9. A method according to claim 8, characterized in that the secondary program consists in disabling the counter (4), in drawing a new random value (R), in initializing the counter (4) with said new value, and in enabling the count-down before returning to the execution of the main program.

10. A method according to claim 8, characterized in that the secondary program can be executed in random time.

11. A method according to claim 10, characterized in that the secondary program consists in disabling the counter (4), in drawing a new random value (R), in counting down to zero from said new random value in a loop of the secondary program, then in drawing another new random value (R), in initializing the counter to said other new value, and in activating the counter, before returning to the execution of the main program.

12. A method according to any one of claims 8 to 11, characterized in that the secondary program also activates current-consuming means.

13. A method according to claim 12, characterized in that said current-consuming means comprise a charge pump (9).

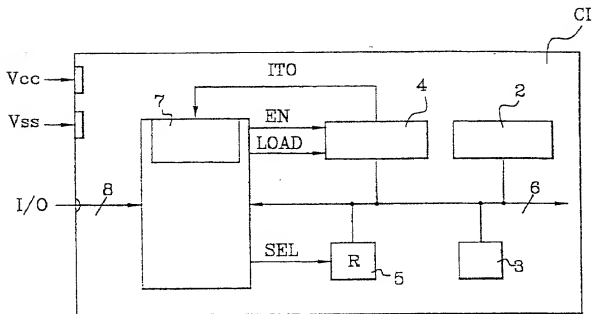
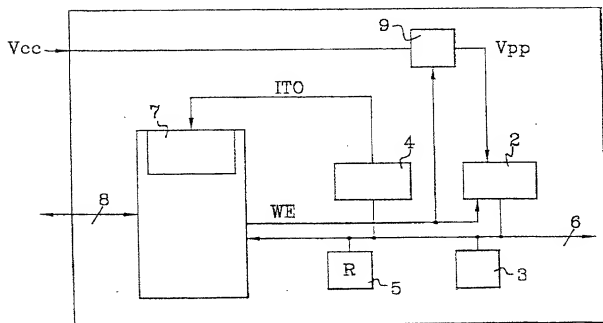
14. A method according to claim 12 or 13, characterized in that said means comprise instructions causing instantaneous current consumption.

5 15. A method according to any one of claims 8 to 14, characterized in that it comprises various secondary programs.

13  
12  
11  
10  
9  
8  
7  
6  
5  
4  
3  
2  
1



1/1

FIG.1FIG.2

**COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY**  
(Includes Reference to Provisional and International (PCT) Applications)

Attorney's Docket No.  
032326-134

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I BELIEVE I AM THE ORIGINAL, FIRST AND SOLE INVENTOR (IF ONLY ONE NAME IS LISTED BELOW) OR AN ORIGINAL, FIRST AND JOINT INVENTOR (IF PLURAL NAMES ARE LISTED BELOW) OF THE SUBJECT MATTER WHICH IS CLAIMED AND FOR WHICH A PATENT IS SOUGHT ON THE INVENTION ENTITLED:

ELECTRONIC COMPONENT FOR MASKING EXECUTION OF INSTRUCTIONS OR DATA MANIPULATION

The specification of which (check only one item below):

- ☐ is attached hereto.  
☒ was filed as United States Patent Application Number 09/807,614  
on April 16, 2001  
and was amended on \_\_\_\_\_ (if applicable).  
☐ was filed as International (PCT) Application Number \_\_\_\_\_  
on \_\_\_\_\_  
and was amended on \_\_\_\_\_ (if applicable).

I HAVE REVIEWED AND UNDERSTAND THE CONTENTS OF THE ABOVE-IDENTIFIED SPECIFICATION, INCLUDING THE CLAIMS, AS AMENDED BY ANY AMENDMENT REFERRED TO ABOVE.

I ACKNOWLEDGE THE DUTY TO DISCLOSE TO THE U.S. PATENT AND TRADEMARK OFFICE ALL INFORMATION KNOWN TO ME TO BE MATERIAL TO PATENTABILITY AS DEFINED IN TITLE 37, CODE OF FEDERAL REGULATIONS, Sec. 1.56 (as amended effective March 16, 1992);

I do not know and do not believe the said invention was ever known or used in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to said application; that said invention was not in public use or on sale in the United States of America more than one year prior to said application; that said invention has not been patented or made the subject of an inventor's certificate issued before the date of said application in any country foreign to the United States of America on any application filed by me or my legal representatives or assigns more than six months prior to said application;

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any International (PCT) Application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT International (PCT) Application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

**PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §119:**

COUNTRY (If PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. §119
France	98/12988	16 October 1998	<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

(APPLICATION NUMBER) (FILING DATE)

(APPLICATION NUMBER) (FILING DATE)

**COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D)**  
(Includes Reference to Provisional and International (PCT) Applications)

Attorney's Docket  
No. 032326-134

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) or International (PCT) Application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations § 1.56, which became available between the filing date of the prior application(s) and the national or international filing date of this application:

PRIOR U.S. APPLICATIONS OR INTERNATIONAL (PCT) APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. § 120:

U.S. APPLICATIONS		STATUS (check one)		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PCT APPLICATIONS DESIGNATING THE U.S.				
PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (if any)		
FR99/02521	15 October 1999			

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the U.S. Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	Eric H. Weisblatt	30,505	Bruce T. Wieder	33,815
Robert S. Swecker	19,885	James W. Peterson	26,057	Todd R. Walters	34,040
Patton N. Mandros	22,124	Teresa Stanek Rea	30,427	Ronni S. Jillions	31,979
Benton S. Duffett, Jr.	22,030	Robert E. Krebs	25,885	Harold R. Brown III	36,341
Norman H. Stepano	22,716	William C. Rowland	30,888	Allen R. Baum	36,086
Ronald L. Grudziecki	24,970	T. Gene Dillahunty	25,423	Steven M. duBois	35,023
Frederick G. Michaud, Jr.	26,003	Patrick C. Keane	32,858	Brian P. O'Shaughnessy	32,747
Allen E. Kopecki	25,813	B. Jefferson Boggs, Jr.	32,344	Kenneth B. Leffler	36,075
Rogée E. Sluiter	26,999	William H. Benz	25,952	Fred W. Hathaway	32,236
Samuel C. Miller, III	27,360	Peter K. Skiff	31,917	Wendi L. Weinstein	34,456
Robert G. Mukai	28,531	Richard J. McGrath	29,195	Mary Ann Dillahunty	34,576
George A. Hovanec, Jr.	28,223	Matthew L. Schneider	33,814		
James A. LaBarre	28,632	Michael G. Savage	32,536		
B. Joseph Cess	28,510	Gerald F. Swiss	30,113		
R. Danny Huntington	27,903	Charles F. Wieland III	33,096		



21839

and: \_\_\_\_\_  
Address all correspondence to: \_\_\_\_\_


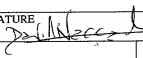
James A. LaBarre  
BURNS, DOANE, SWECKER & MATHIS, L.L.P.  
P.O. Box 1404  
Alexandria, Virginia 22313-1404



21839

Address all telephone calls to: James A. LaBarre at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

<b>COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D)</b> (Includes Reference to Provisional and International (PCT) Applications)		Attorney's Docket No. 032326-134	
FULL NAME OF SOLE OR FIRST INVENTOR Philippe ANGUIA		SIGNATURE 	DATE 03-05-2001
RESIDENCE (CITY & STATE/COUNTRY) 227, chemin de Riquet, F-13400 Aubagne, FRANCE FRX		CITIZENSHIP France	
POST OFFICE ADDRESS (HOME ADDRESS) 227, chemin de Riquet, F-13400 Aubagne, FRANCE			
FULL NAME OF SECOND JOINT INVENTOR, IF ANY David NACCACHE		SIGNATURE 	DATE 11-06-2001
RESIDENCE (CITY & STATE/COUNTRY) 7, rue Chaptal, F-75009, Paris, FRANCE FRX		CITIZENSHIP France	
POST OFFICE ADDRESS (HOME ADDRESS) 7, rue Chaptal, F-75009, Paris, FRANCE			
FULL NAME OF THIRD JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)			
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)			
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)			
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)			
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)			
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)			
FULL NAME OF NINTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)			
FULL NAME OF TENTH JOINT INVENTOR, IF ANY		SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)		CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)			